CERT

Insider Threats and Security Trends: Lessons Learned from Actual Insider Attacks

Adam Cummings
Randy Trzeciak

CERT Insider Threat Center

http://www.cert.org/insider_threat/

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

ACTUAL CASE

A federal agency’s former database administrator wipes out all critical data in their mission critical database…

The agency’s systems are down for 3 days while 115 employees spend 1800 hours to recover & re-enter the data.

Agenda

Introduction

How bad is the insider threat?

Background on SEI , CERT and our insider threat research

Exploration of each type of insider crime

Mitigation Strategies for Prevention and Detection

DHS Insider Threat Assessment

Discussion

Introduction

What is CERT?

Center of Internet security expertise

Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Located in the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

CERT Insider Threat Center—Mission

Assist organizations in identifying indications and warnings of insider threat by

- performing vulnerability assessments
- assisting in the design and implementation of policies, practices, and technical solutions

based on our ongoing research of hundreds of actual cases of insider IT sabotage, theft of intellectual property, fraud, and espionage

Who is a Malicious Insider?

Current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization’s network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.*

How bad is the insider threat?

e-Crime Watch Survey

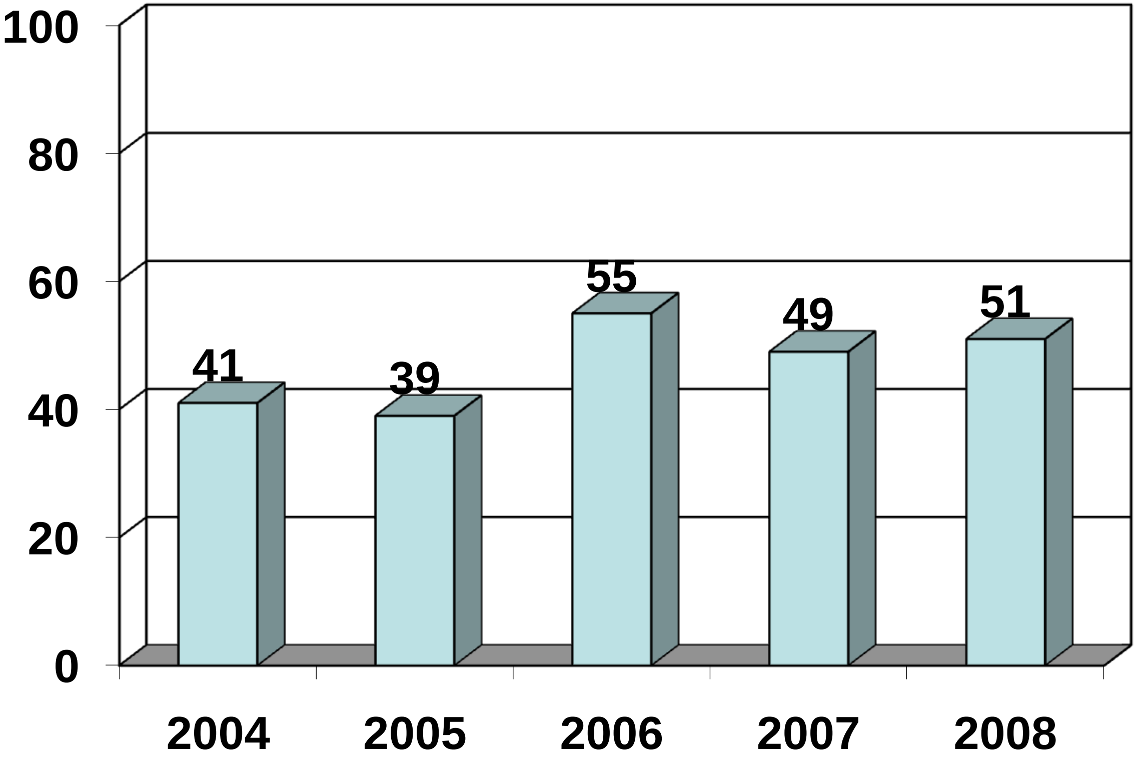
CSO Magazine, USSS, CERT & Deloitte

523 respondents

39% of organizations have less than 500 employees

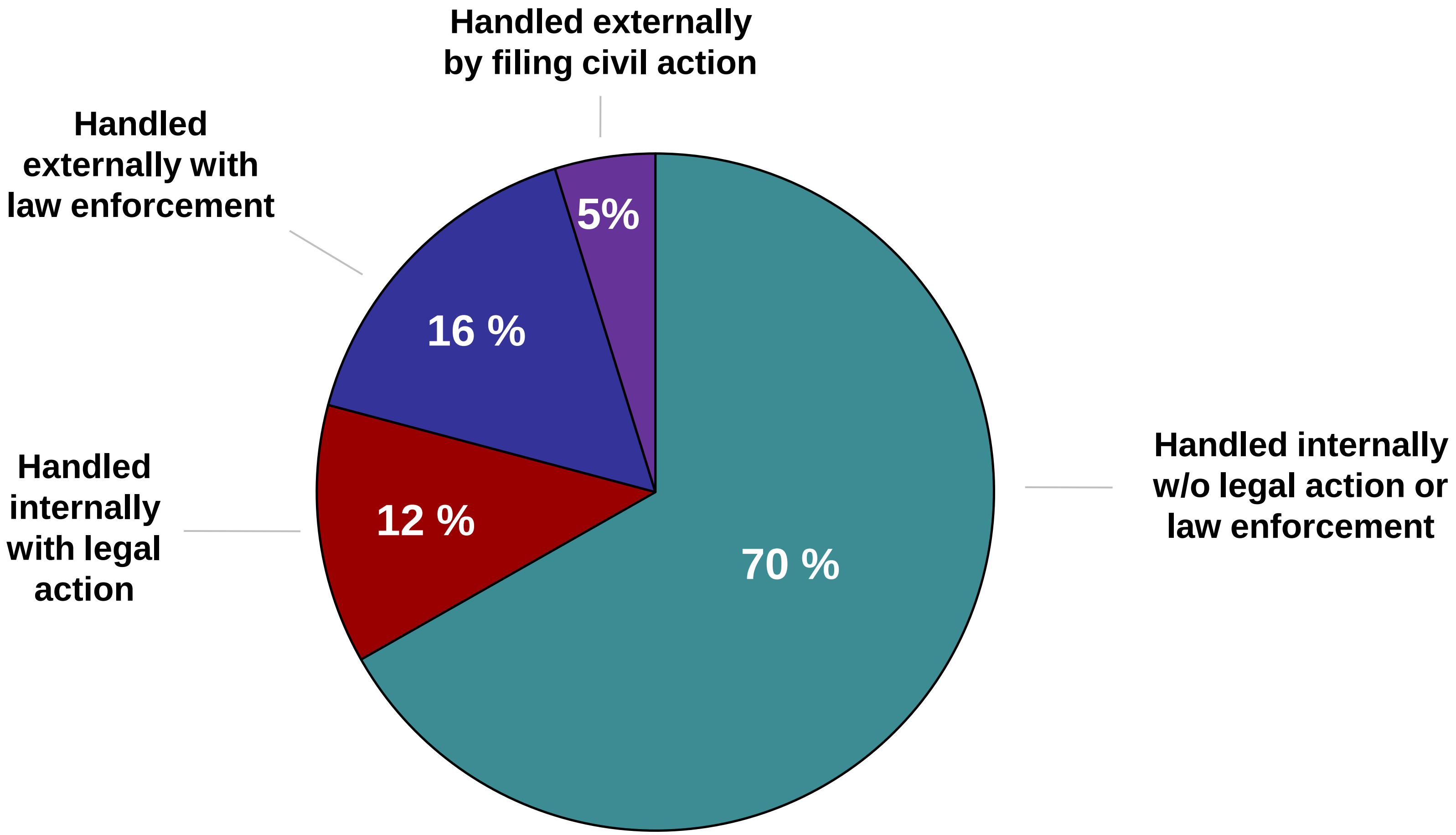
23% of organizations have less than 100 employees

Percentage of Participants Who Experienced an Insider Incident



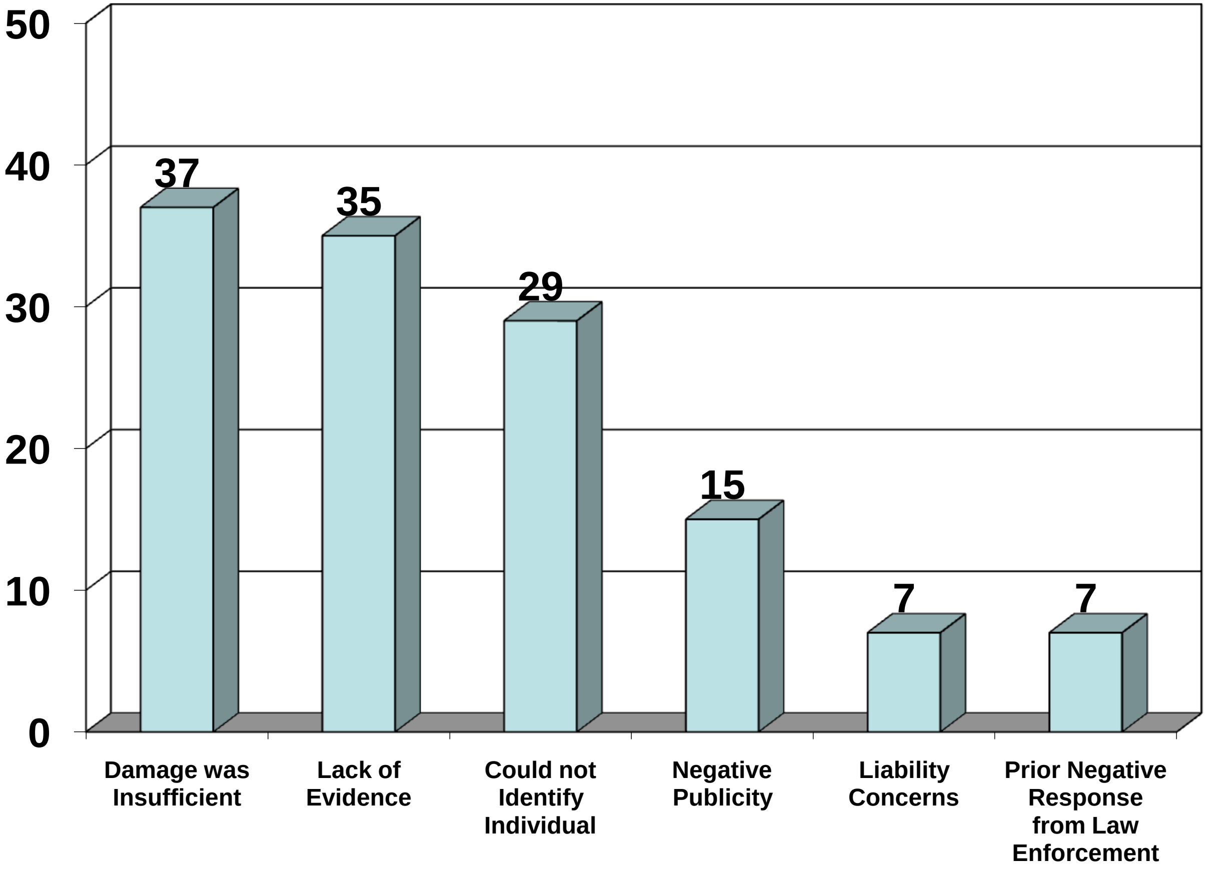
e-Crime Watch Survey - 2

Which percentage of Electronic Crimes committed by insiders were:



2009 E-Crime Survey Results

Reasons cyber security events were not referred for legal action

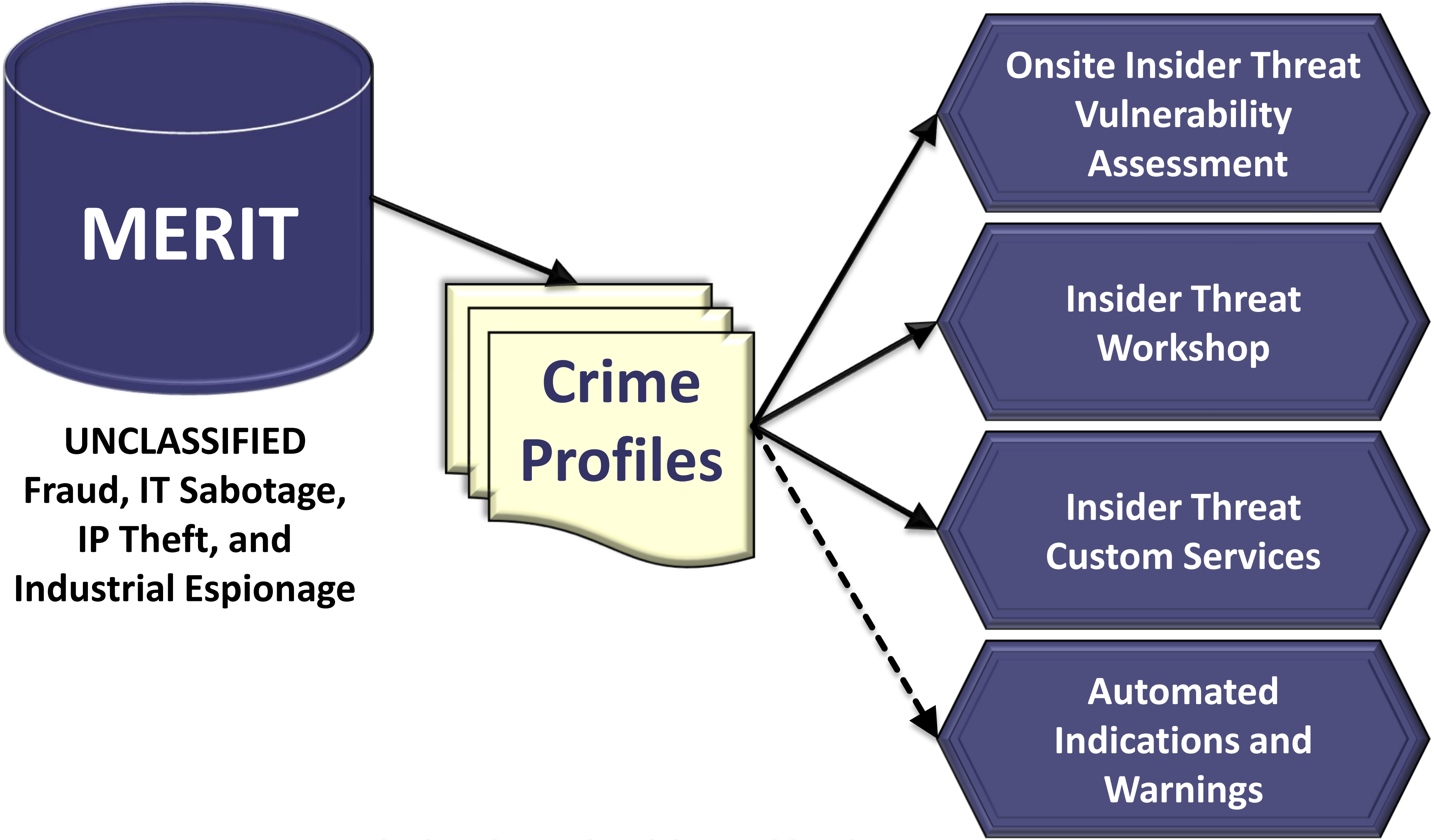


The Expanding Complexity of "Insiders"

Area	Description
Collusion with outsiders	Insiders recruited by or working for outsiders, including organized crime and foreign organizations or governments
Business partners	Difficulty in controlling/monitoring access to your information and systems by "trusted" business partners
Mergers & acquisitions	Heightened risk of insider threat in organizations being merged into acquiring organization
Cultural differences	Difficulty in recognizing behavioral indicators exhibited by insiders working for US organizations who are not US citizens
Foreign allegiances	US organizations operating branches outside the US with the majority of employees who are not US citizens

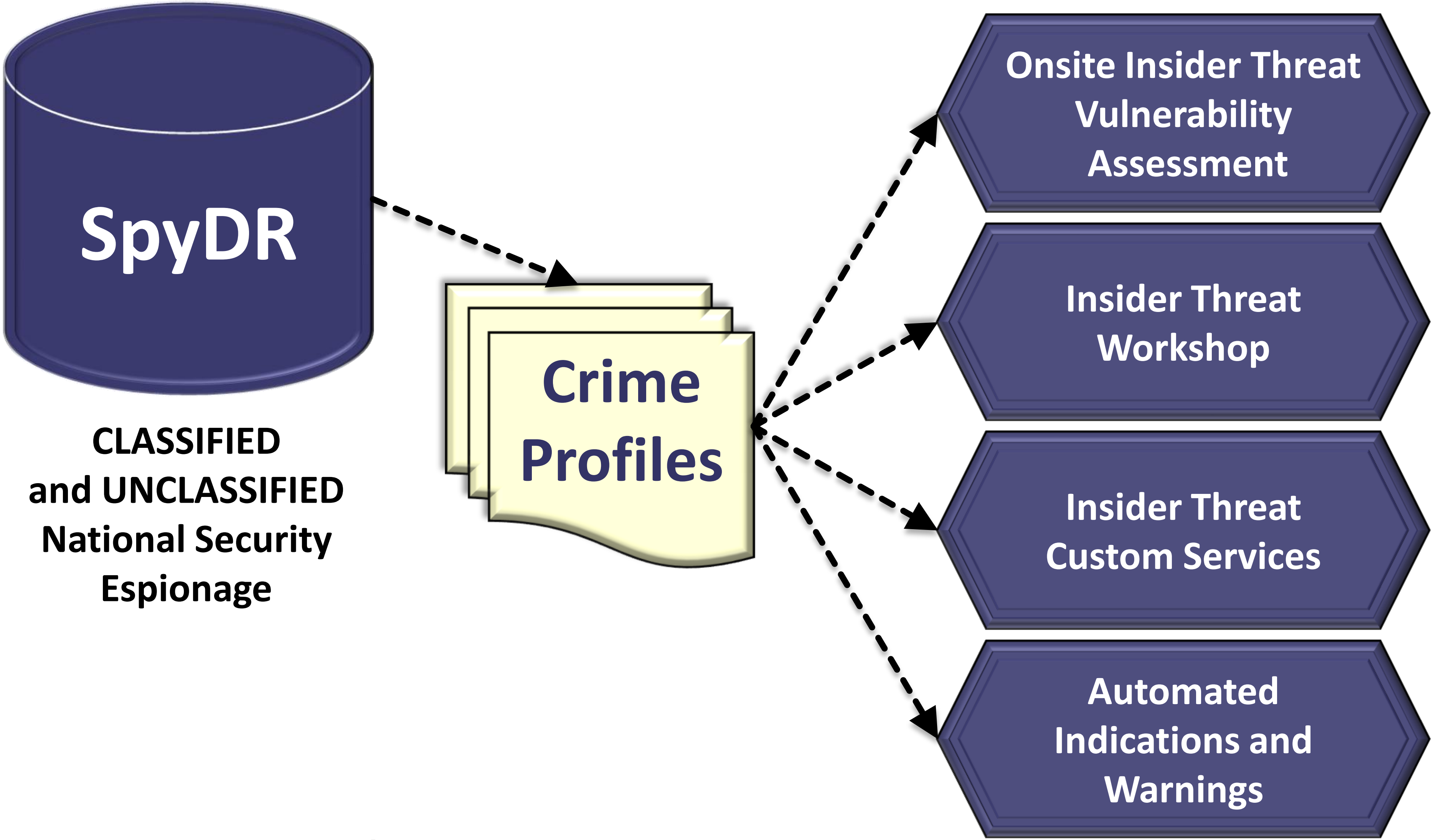
CERT's Insider Threat Research

CERT's Insider Threat Portfolio


MERIT
UNCLASSIFIED
Fraud, IT Sabotage,
IP Theft, and
Industrial Espionage
Crime Profiles
Onsite Insider Threat Vulnerability Assessment
Insider Threat Workshop
Insider Threat Custom Services
Automated Indications and Warnings

MERIT – Management and Education of the Risk of Insider Threat

CERT’s Insider Threat Portfolio



SpyDR

CLASSIFIED
and UNCLASSIFIED
National Security
Espionage

Crime Profiles

Onsite Insider Threat Vulnerability Assessment

Insider Threat Workshop

Insider Threat Custom Services

Automated Indications and Warnings

SpyDR– Spy Data Repository

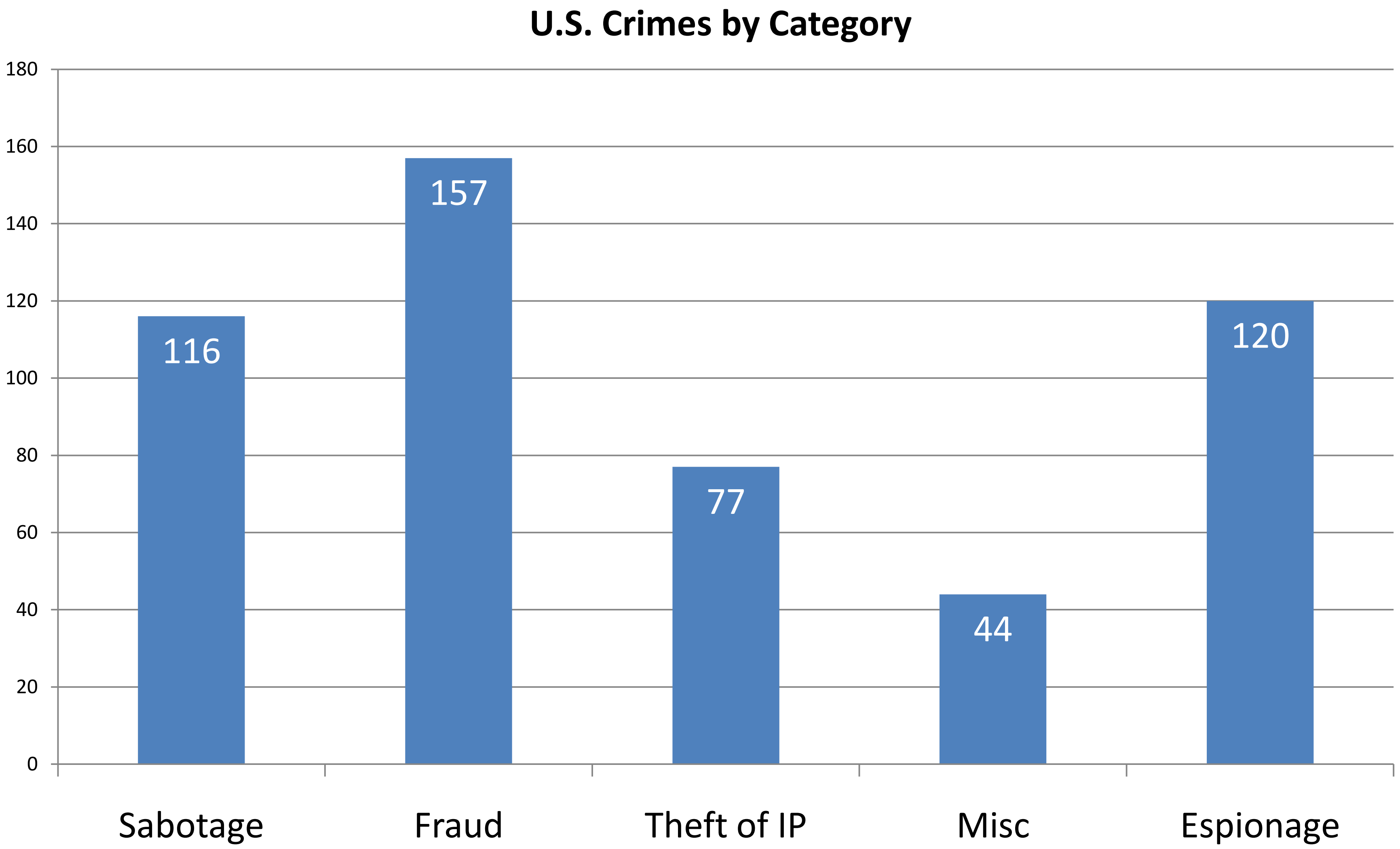
Types of Insider Crimes

Sabotage: An insider’s use of IT to direct specific harm at an organization or an individual.

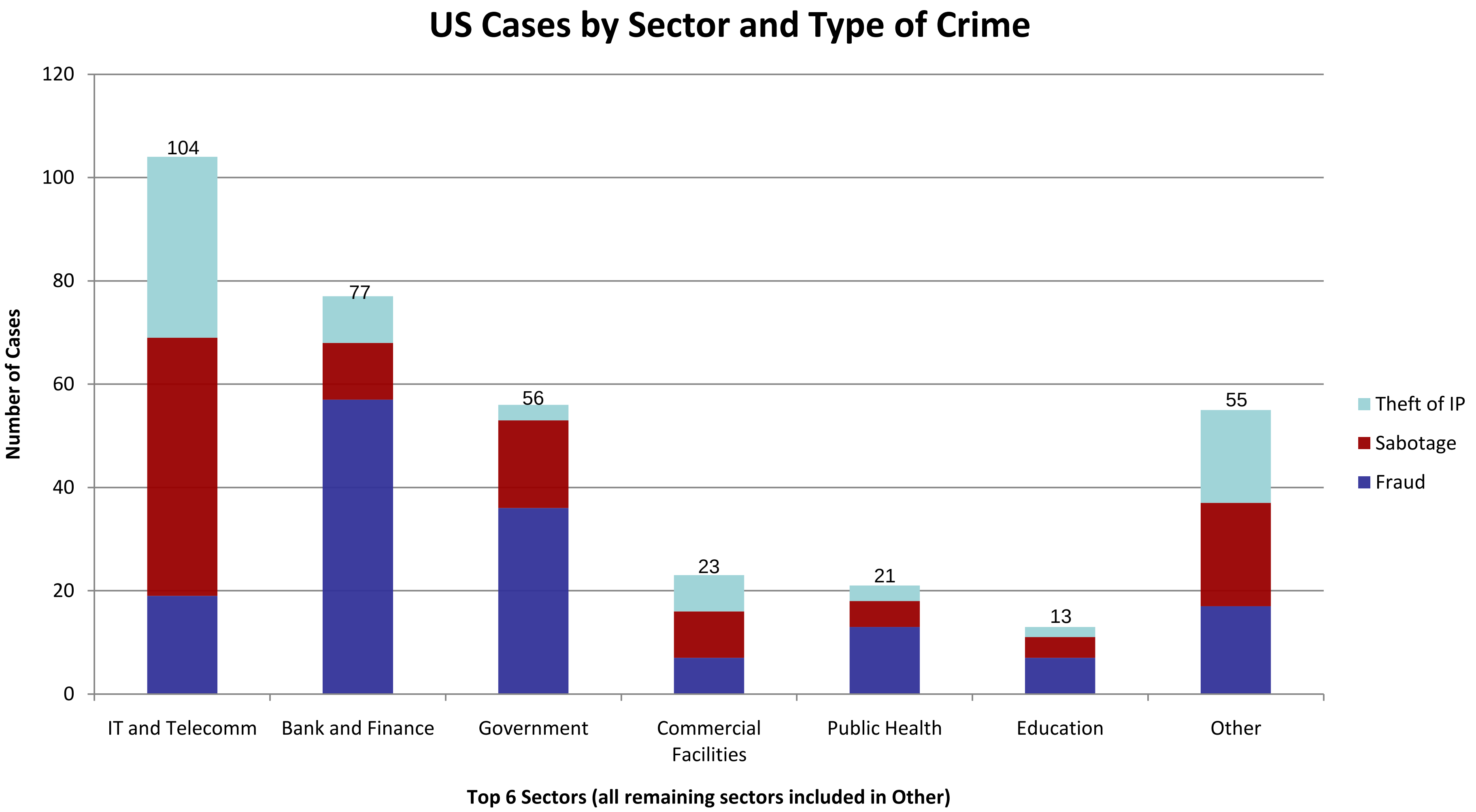
Theft of intellectual property: An insider’s use of IT to steal confidential or sensitive information from the organization.

Fraud: An insider’s use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).

CERT's Insider Threat Case Database



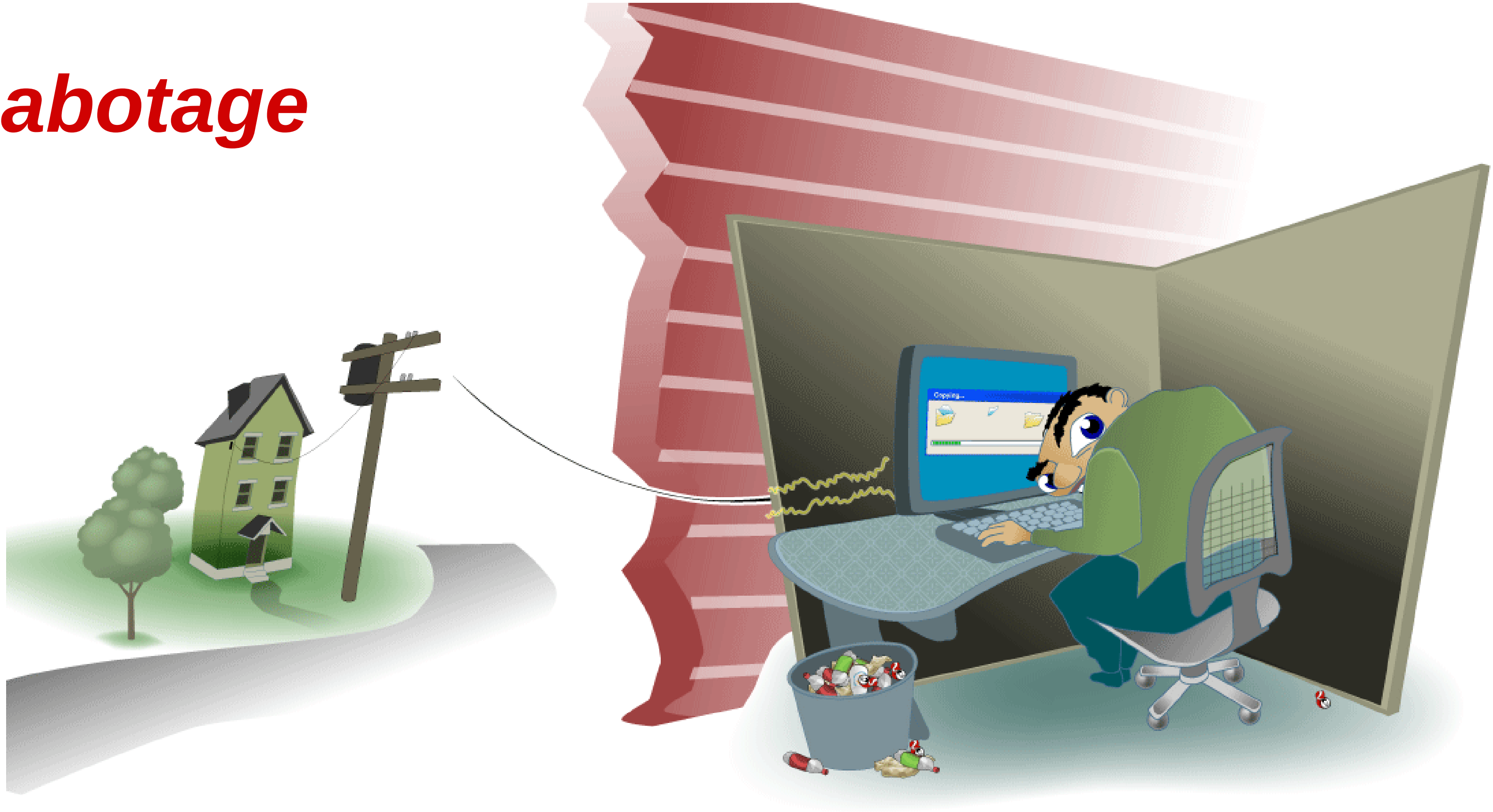
Critical Infrastructure Sectors



Brief Overview of Findings From Our Research

Scenario 1:

IT Sabotage



Insider IT Sabotage

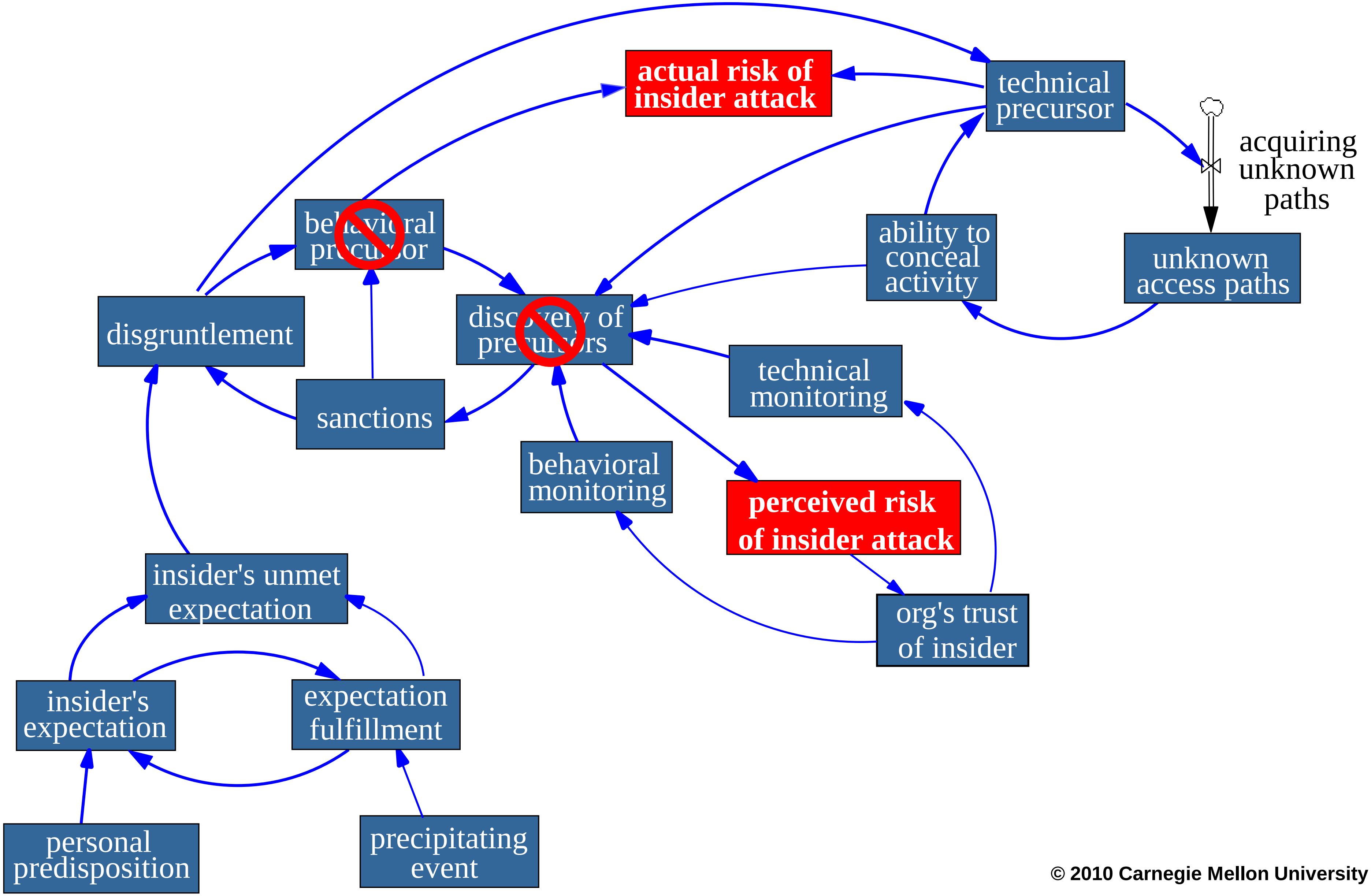
Who did it?

- Former employees
- Male
- Highly technical positions
- Age: 17 – 60

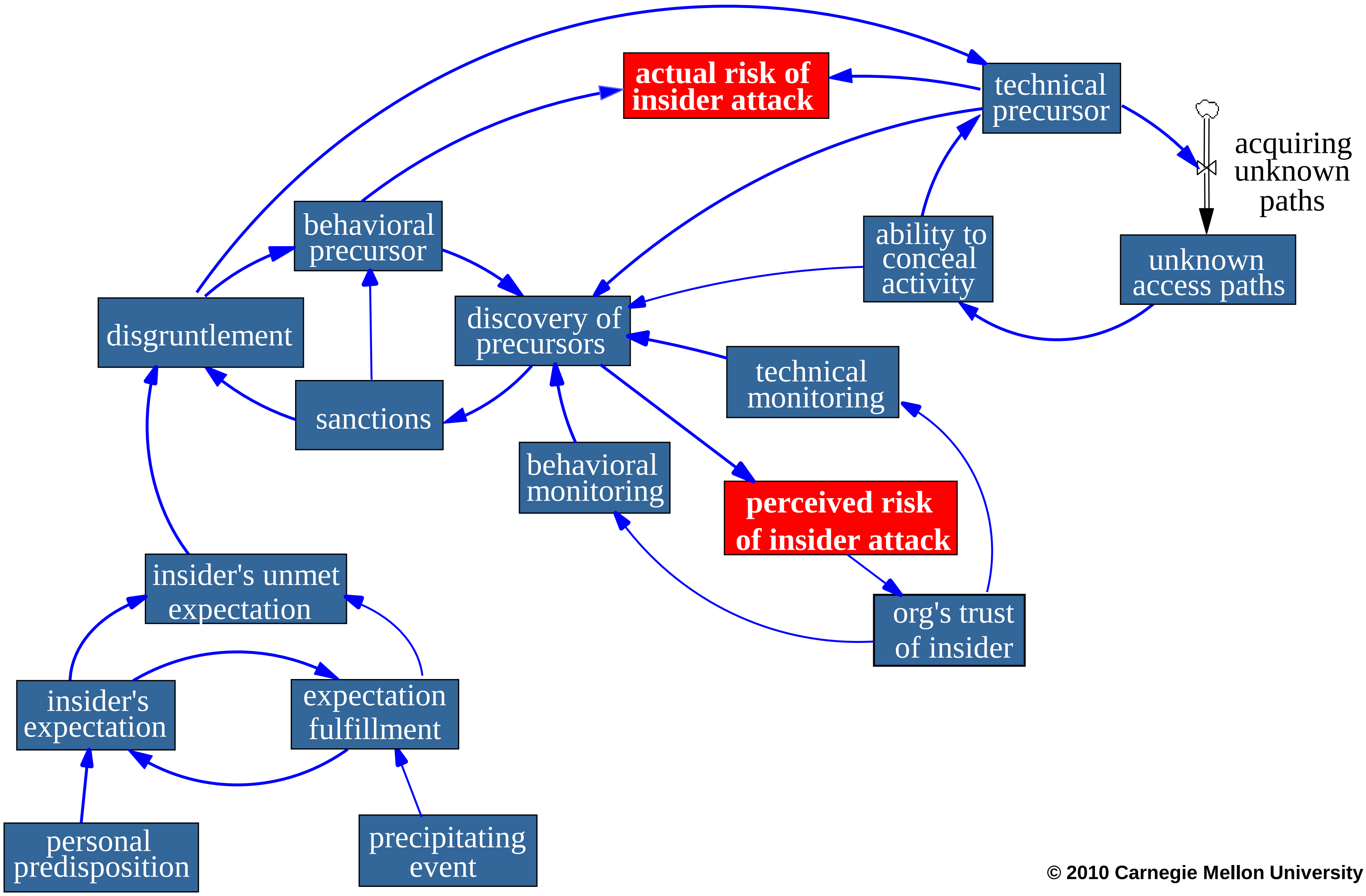
How did they attack?

- No authorized access
- Backdoor accounts, shared accounts, other employees’ accounts, insider’s own account
- Many technically sophisticated
- Remote access outside normal working hours

MERIT Model of Insider IT Sabotage



MERIT Model of Insider IT Sabotage



Scenario 2:

Theft of Intellectual Property

WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
CONFIDENTIAL
RESEARCH
PATENTS

Theft of Intellectual Property

Who did it?

- Current employees
- Technical or sales positions
- All male
- Average age: 37

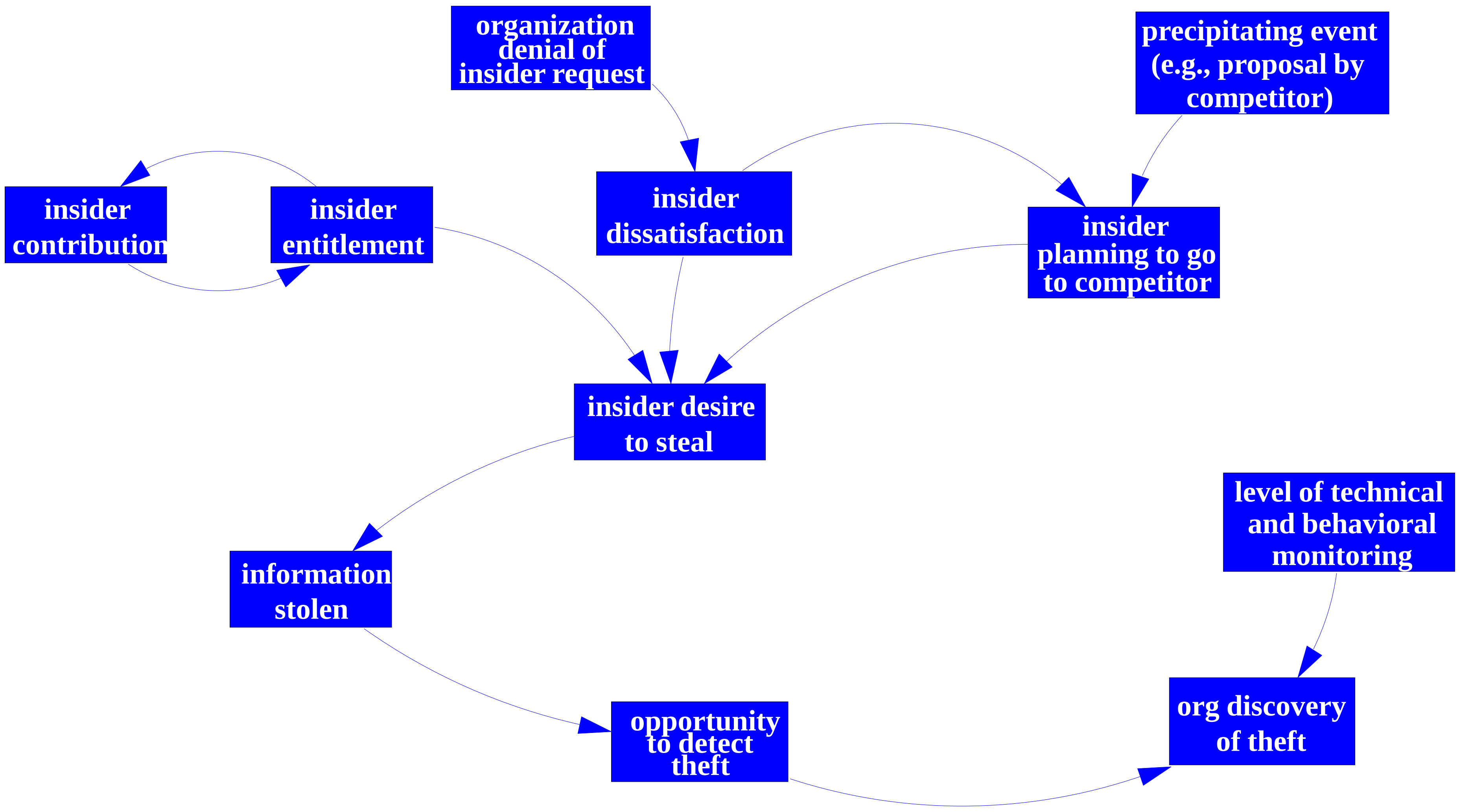
What was stolen?

- Intellectual Property (IP)
- Customer Information (CI)

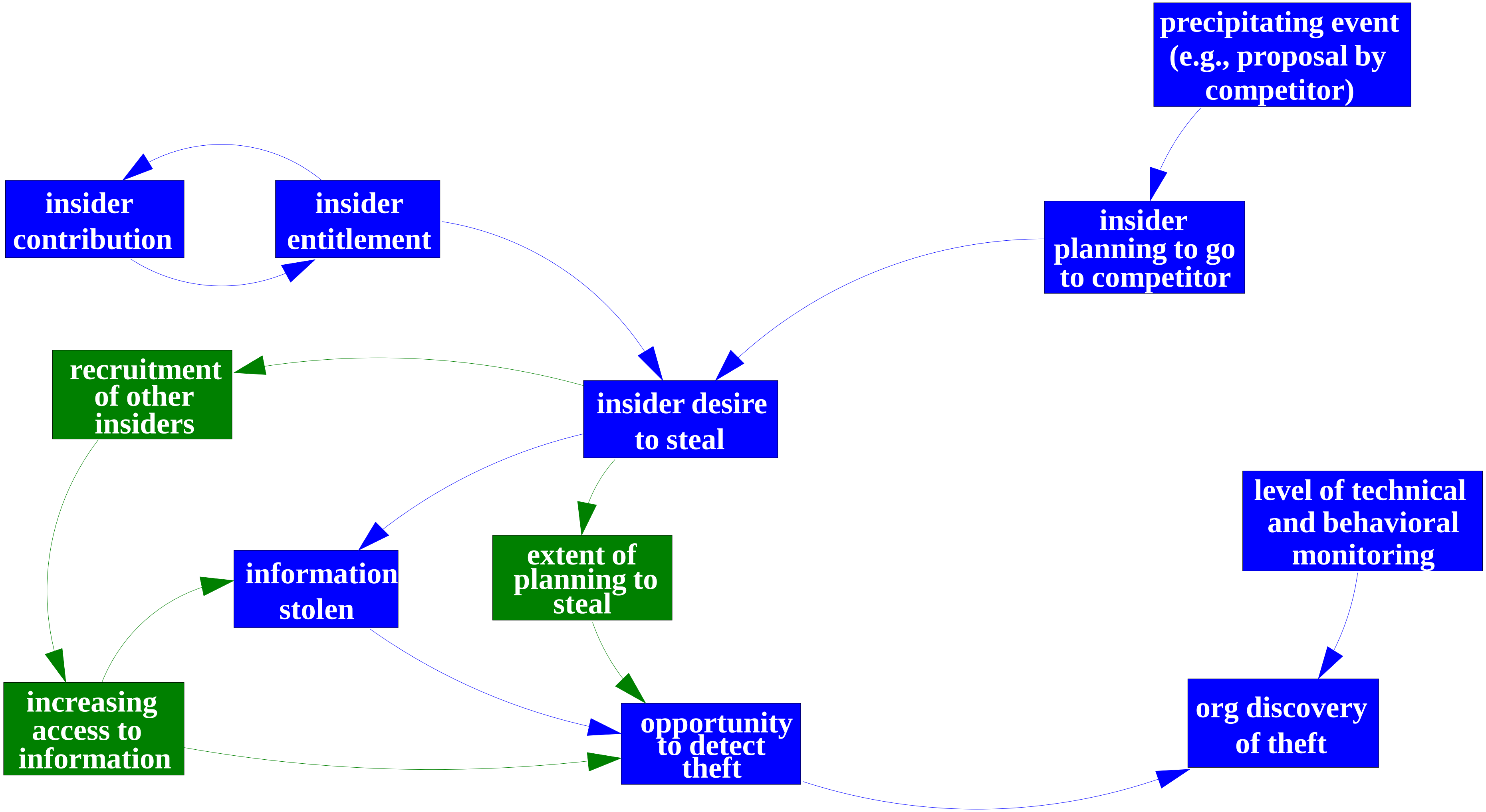
How did they steal it?

- During normal working hours
- Using authorized access

MERIT Model of Insider Theft of IP – Entitled Independent


organization denial of insider request
precipitating event (e.g., proposal by competitor)
insider contribution
insider entitlement
insider dissatisfaction
insider planning to go to competitor
insider desire to steal
level of technical and behavioral monitoring
information stolen
org discovery of theft
opportunity to detect theft

MERIT Model of Insider Theft of IP – Ambitious Leader


precipitating event (e.g., proposal by competitor)
insider contribution
insider entitlement
insider planning to go to competitor
recruitment of other insiders
insider desire to steal
level of technical and behavioral monitoring
information stolen
extent of planning to steal
increasing access to information
opportunity to detect theft
org discovery of theft

Dynamics of the Crime

Most were *quick* theft upon resignation

Stole information to

- Take to a new job
- Start a new business
- Give to a foreign company or government organization

Collusion

- Collusion with at least one *insider* in almost 1/2 of cases
- Outsider *recruited* insider in less than 1/4 of cases
- Acted *alone* in 1/2 of cases

Known Issues

Disagreement over ownership of intellectual property

Financial compensation issues

Relocation issues

Hostile work environment

Mergers & acquisitions

Company attempting to obtain venture capital

Problems with supervisor

Passed over for promotion

Layoffs

Technical Aspects – Theft of Intellectual Property

In order of prevalence:

- Copied/downloaded information
- Emailed information
- Accessed former employer’s system
- Compromised account

Many other methods

Scenario 3:

Fraud

Fraud

Who did it?

- Current employees
- “Low level” positions
- Gender: fairly equal split
- Average age: 33

What was stolen/modified?

- Personally Identifiable Information (PII)
- Customer Information (CI)
- Very few cases involved trade secrets

How did they steal/modify it?

- During normal working hours
- Using authorized access

Dynamics of the Crime

Most attacks were long, ongoing schemes

	At least 1 Insider Colluder	*At least 1 Outsider Colluder*	*Outsider Induced*	*Acted Alone*
Theft	almost 1/3	2/3	1/2	> 1/3

Technical Aspects - Fraud

Electronically

- Downloaded to home
- Looked up and used immediately
- Copied
- Phone/fax
- Email
- Malicious code

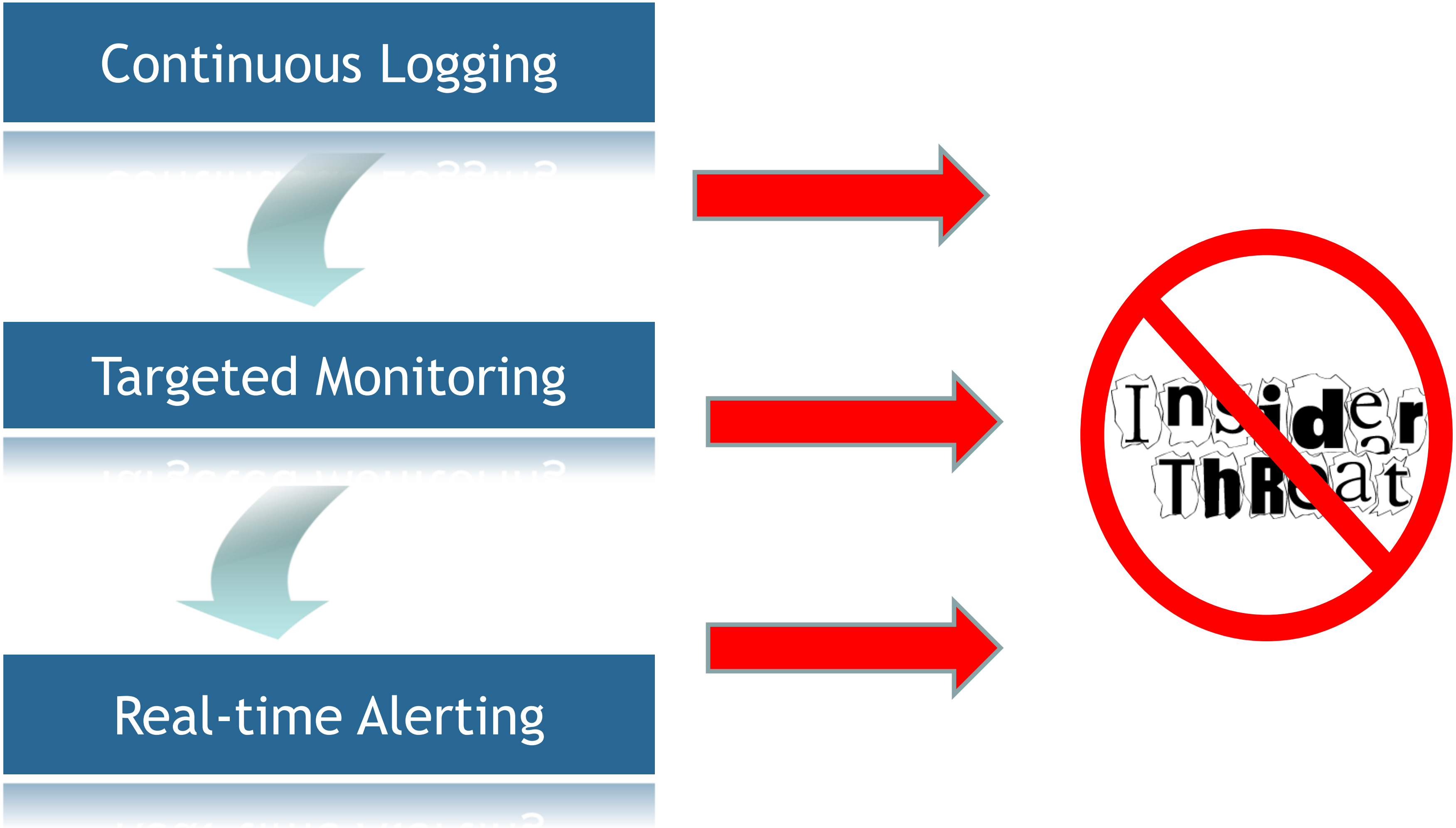
Physically

- Printouts
- Handwritten

Remaining unknown

Mitigation Strategies

Our Suggestion



Continuous Logging

Targeted Monitoring

Real-time Alerting

Summary of Best Practices

- Consider threats from insiders and business partners in enterprise-wide risk assessments.
- Clearly document and consistently enforce policies and controls.
- Institute periodic security awareness training for all employees.
- Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.
- Anticipate and manage negative workplace issues.
- Track and secure the physical environment.
- Implement strict password and account management policies and practices.
- Enforce separation of duties and least privilege.
- Consider insider threats in the software development life cycle.
- Use extra caution with system administrators and technical or privileged users.
- Implement system change controls.
- Log, monitor, and audit employee online actions.
- Use layered defense against remote attacks.
- Deactivate computer access following termination.
- Implement secure backup and recovery processes.
- Develop an insider incident response plan.

DHS Insider Threat Assessment

MERIT Insider Threat Vulnerability Assessment

Objective: Leverage what we’ve learned to create actionable guidance for organizations to mitigate insider threats to their organization.

Method: Document Review, Process Observation, and Onsite interviews using insider threat vulnerability assessment workbooks based on all insider threat *areas of concern* in all cases in the CERT case library.

Outcome: Confidential report of findings detailing organizational issues of concern, prevalence of each issue in the cases, mitigation strategies, and relative difficulty/cost for each countermeasure.

Scope of Vulnerability Assessment

Addresses all types of vulnerabilities exploited in the cases we have studied

- Technical
- Psychological
- Process
- Policy

- IT Sabotage
- Theft of Information
- Fraud

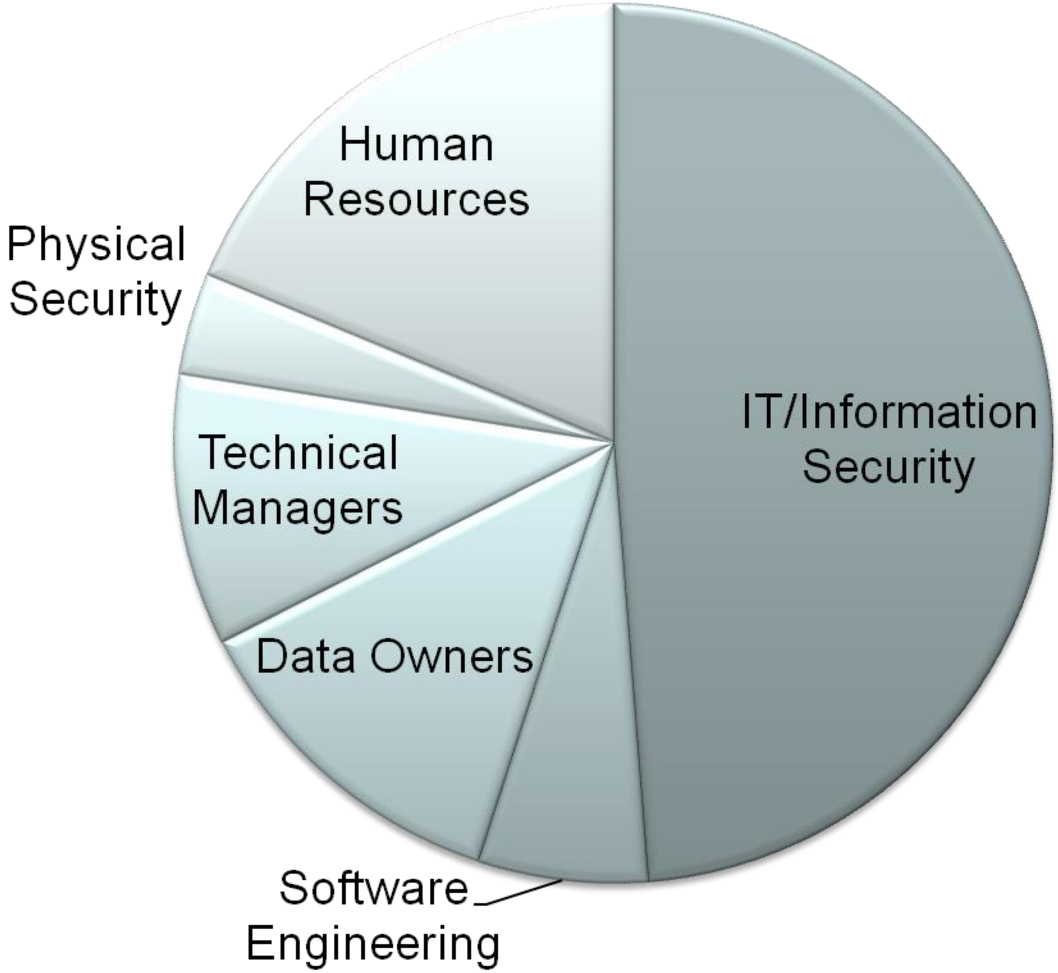
Site visit by CERT– includes interviews with stakeholders:

- Information Technology / Information Security
- Human Resources
- Physical Security
- Software Engineering
- Data “Owners”
- Legal

CERT Insider Threat Vulnerability Assessment

Addresses all types of vulnerabilities exploited in the cases we have studied

- Technical
- Psychological
- Process
- Policy



Discussion

Publicly Available Information

Reports

- Protecting Against Insider Threat
- Common Sense Guide to Prevention and Detection of Insider Threats, Version 3.1
- Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis

Podcasts

- Insider Threat and the Software Development Life Cycle
- Protecting Against Insider Threat
- CERT Execs on the 2006 E-Crime Watch Survey

Insider Threat Study

- Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector
- Insider Threat Study: Illicit Cyber Activity in the Government Sector
- Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors
- Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector

System Dynamics

- An Experience Using System Dynamics to Facilitate an Insider Threat Workshop
- Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage

E-Crime Watch Survey

- 2008, 2007, 2006, 2005, 2004

Available at: http://www.cert.org/insider_threat/

Points of Contact

Insider Threat Center @ CERT
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

Randy Trzeciak
Insider Threat Team Lead
412 268-7040
rft@cert.org

Adam Cummings
Insider Threat Project Lead
412 268-9004
abc@cert.org

http://www.cert.org/insider_threat/

Insider Threat